

PathResolve

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3344 bytes

Attack Category	<ul style="list-style-type: none">• Malicious Input		
Vulnerability Category	<ul style="list-style-type: none">• Buffer Overflow• Unconditional		
Software Context	<ul style="list-style-type: none">• File Path Management		
Location	<ul style="list-style-type: none">• shlobj.h		
Description	<p>The destination string buffer for PathResolve() must be long enough to hold the fully qualified path.</p> <p>The PathResolve() routine converts a relative path to a fully qualified pathname. It modifies the path parameter in place.</p>		
APIs	Function Name	Comments	
	PathResolve		
Method of Attack	<p>The pszPath variable is modified in place to contain the fully qualified path. If the attacker provides a relative path to a very long path name, this could overflow the buffer. Furthermore, if the string buffer is declared exactly the size of the input string, a buffer overflow is almost guaranteed to occur.</p>		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Whenever PathResolve() is called.	The first parameter, pszPath, must be at least MAX_PATH characters in length.	Effective
Signature Details	BOOL PathResolve(LPWSTR pszPath, LPCWSTR *dirs, UINT fFlags);		

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

Examples of Incorrect Code	<pre> WCHAR path[] = L"MyFile.dat"; // Buffer is too small LPWSTR pszPath = path; LPCWSTR dirs[] = { NULL }; if (!PathResolve(pszPath, dirs, PRF_VERIFYEXISTS) { handleError(); } </pre>	
Examples of Corrected Code	<pre> WCHAR path[MAX_PATH] = L"MyFile.dat"; // Buffer is correctly sized LPWSTR pszPath = path; LPCWSTR dirs[] = { NULL }; if (!PathResolve(pszPath, dirs, PRF_VERIFYEXISTS) { handleError(); } </pre>	
Source Reference	<ul style="list-style-type: none"> • http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/pathresolve.asp² 	
Recommended Resource		
Discriminant Set	Operating System	<ul style="list-style-type: none"> • Windows
	Languages	<ul style="list-style-type: none"> • C • C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>